

# CYBERSECURITY CLASSES AND CERTIFICATIONS

## CERTIFIED CYBERSECURITY ENTRY-LEVEL TECHNICIAN (PCCET)

Prepare to take this certification exam by taking the following four courses.

### Cybersecurity Foundation – \$600 (48 hours)

In the Cybersecurity Foundation course, students will learn fundamental principles associated with the current cybersecurity landscape and identify concepts required to recognize and potentially mitigate attacks against enterprise networks as well as mission critical infrastructure. Students will also learn how to initially setup and configure interfaces, security zones, authentication, and policies on a next generation firewall.

### Network Security Fundamentals – \$600 (48 hours)

In the Network Security Fundamentals course, students will gain an understanding of the fundamental tenants of network security and review the general concepts involved in maintaining a secure network computing environment. Upon successful completion of this course, students will be able to describe general network security concepts and implement basic network security configuration techniques.

### Security Operations Fundamentals – \$600 (48 hours)

In the Security Operations Fundamentals course, students will gain an understanding of Security operations (SecOps) and the

role it plays in protecting our digital way of life, for businesses and customers. Students will learn continuous improvement processes to collect high-fidelity intelligence, contextual data, and automated prevention workflows that quickly identify and respond to fast-evolving threats. They will also learn how to leverage automation to reduce strain on analysts and execute the Security Operation Center's (SOC) mission to identify, investigate, and mitigate threats.

### Cloud Security Fundamentals – \$600 (48 hours)

In the Cloud Security Fundamentals course, students will learn basic principles associated with securing the cloud and SaaS-based applications through Secure Access Service Edge architecture and identify concepts required to recognize and potentially mitigate attacks against traditional and hybrid data centers as well as mission critical infrastructure. Students will also learn how to initially setup and configure containers on a docker bridge network and test the container security through the use of vulnerability scans and reports.

## CERTIFIED NETWORK SECURITY ADMINISTRATOR (PCNSA)

Prepare to take this certification exam by taking the following two courses.

### Cybersecurity Infrastructure Configuration – \$600 (48 hours)

Students will learn to configure the security, networking, threat prevention, logging, and reporting features of next generation firewall technologies.

### Cybersecurity Prevention and Countermeasures – \$600 (48 hours)

Students will learn to configure traffic handling, advanced content/user identification, quality of service, global protect, monitoring/reporting, and high availability of next generation firewall technologies



Offered online at [bismarckstate.edu/CybersecurityCertifications](https://bismarckstate.edu/CybersecurityCertifications)

To learn more call 701-224-5600